Maryland Virtualization Policy

Last Updated: 05/30/2017

Contents

1.0 Purpose

Organizations, including government agencies, are increasingly virtualizing servers and desktops to gain efficiency. The State's use of **virtualization** technology creates security challenges that must be addressed when deploying, migrating, administering, and retiring virtual machines. The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of the Executive Branch of Maryland State government Information Technology (IT) networks, systems, applications, and data.

This policy establishes the information security requirements for virtualization, utilizing the standards identified in NIST SP 800-53R4, SP 800-125, as well as industry best practices.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 8: Virtualization Technologies and any policy regarding virtualization declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
05/30/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

All Executive Branch agencies deploying or implementing virtualization technologies, such as server and desktop virtualization, will ensure risks to data loss or compromise are mitigated by operating in accordance with the requirements described in section 4.0 below.

4.0 Policy

The State of Maryland strives to implement efficient business processes and cost-beneficial technology solutions to provide the best possible services to its constituency. Agencies are increasingly using virtualization to gain operational efficiency. Virtualization offers an agency the ability to streamline agency functions using existing or new hardware purchases.

Virtualization also adds layers of technology which can create vulnerabilities and requires additional security controls to mitigate the ability to exploit weaknesses.

This policy applies to all **Full Virtualization** capabilities, whether:

- **Native Virtualization**; or
- **Hosted Virtualization**.

The requirements described below will allow agencies to:

- Identify and control how **confidential data** is, or may be, accessed, modified, or stored through a virtual environment

- Ensure accountability through authentication controls
- Ensure virtualized solutions are accounted for in the asset management and configuration management processes
- Utilize tools to monitor for malicious activity and to help prevent data loss or compromise

If all four of these capabilities cannot be enabled, agencies should not deploy virtualized environments or assets with the ability to access any confidential information.

4.1 General Requirement for Dedicated (Hardware) Hosts

All hardware in a full-virtualization environment should be dedicated to the virtualization with only virtual implementations allowed; no non-virtual systems or applications will be allowed to share the virtualization host. The host should be configured to meet the security requirements of the highest security classification of all its supported guests.

For example, if one guest provides a critical service that is considered high confidentiality, then the host must be configured to protect that classification level. Guests who require moderate or low confidentiality cannot be guests on that host unless their security controls are also implemented at the high level, thereby minimizing the ability of a less secure guest to be compromised and impact critical guests or the physical host.

Additional security requirements for **hypervisor** and guest **operating system (OS)** security, including virtualization system development lifecycle practices, are outlined in sections 4.2 – 4.4 below.

4.2 Hypervisor Security

Agencies handle a variety of data with varying classification levels requiring different security controls. Substantial security risks can be incurred when consolidating multiple services or data stores with differing classification levels within a single hypervisor. Therefore, as with securing a host, the hypervisor must also be configured to meet the security requirements of the highest-security-classification guest.

Generally, the hypervisor should be secured using the same methods as those used to protect software running on desktops and servers. Because of the hypervisor's level of access to and control over **guest OSs**, implementing security controls on the hypervisor helps prevent confidential data loss and limits the ability of an adversary to take control of *all* the guests.

Access to the virtualization management system should be restricted to authorized administrators only. It is important to secure each hypervisor management interface, both locally and remotely, and to restrict remote administration interfaces through the firewall. Detailed security controls related to hypervisor security are listed in the table below.

#	Name	Requirement
A	Patch Management	Install all updates to the hypervisor that are released by the vendor. Use centralized patch management solutions to administer updates, where applicable.

#	Name	Requirement
B	Restrict Access	▪ Restrict administrative access to the management interfaces of the hypervisor ▪ Follow all the security policies for access control, authentication, elevated privilege, and least privilege as for any hardware-based system
C	Encrypt Communication	Protect all management communication channels by either method below: ▪ Use a dedicated management network ▪ Authenticate and encrypt management network communications using FIPS 140-2 validated cryptographic modules
D	Asset Management	Create, deploy, and manage virtual machines (VMs) in accordance with the *Asset Management Policy*.
E	Configuration	Hypervisor should be secured to the level of classification required by the highest-requirement guest OS.
F	Configuration Management	Centralize configuration management of hypervisors and follow configuration management processes to ensure that all configurations (e.g., high risk, medium risk, and low risk) are documented.
G	Synchronization	Synchronize the virtualized infrastructure to a trusted authoritative time server.
H	Disconnect Unused Hardware	Disconnect unused physical hardware from the host system.
I	Disable Unneeded Services	Disable all hypervisor services, such as clipboards – or file sharing between the guest OS and the **host operating system (host OS)** – unless they are needed.
J	Monitoring Capabilities	Consider monitoring security indicators of: ▪ Each guest OS ▪ Activity occurring between guest OSs NOTE: This capability may have to be done through host-based security controls as network traffic between guest OSs may not pass through network-based security controls.
K	Test and Production Environment	Separate production from test environments. Every host should be designated as belonging to either a production or the test environment, and all "work" on every host should maintain that separation.
L	Monitor Hypervisor	Carefully monitor the hypervisor itself for signs of compromise. This may include: ▪ Using self-integrity monitoring capabilities that hypervisors may provide ▪ Monitoring and analyzing hypervisor logs on an ongoing basis

4.3 Guest OS Security

The operating system of a virtual machine instantiated on a virtual server (i.e., a hypervisor) is referred to as a "guest" OS. All the security considerations that apply to OSs running on real hardware also apply to guest OSs; however, there are some additional security considerations. Agencies must apply and enforce the controls listed in the table below to ensure that guest OSs meet security configuration requirements and do not increase the risk of compromise for fellow guests.

#	Name	Requirement
A	Policy Application	Follow all recommended practices in DoIT Cybersecurity Policies for managing physical OSs, including but not limited to: ▪ Log management ▪ Authentication requirements ▪ Remote access controls
B	Configuration	No guest OS shall be secured at a higher security classification than its hypervisor.
C	Configuration Management	Centralize configuration management of guest OSs and follow configuration management processes to ensure that all configurations (e.g., high risk, medium risk, and low risk) are documented.
D	Patch Updates	Install all patch updates to the guest OS promptly, according to the DoIT *Patch Management Policy* and processes.
E	Backups	Back up all the virtual drives used by the guest OS on a regular schedule, using the same process for backups as is used for non-virtualized computers in the organization (See *Contingency Planning Policy*).
F	Disconnect Unused Hardware	Disconnect unused virtual hardware in each guest OS.
G	Authentication Methods	Use separate authentication credentials for each OS unless there is a particular reason for two guest OSs to share credentials.
H	Association	Ensure that virtual devices for the guest OS are associated only with the appropriate physical devices on the host system, such as the mapping between virtual network interface cards (NICs) to the proper physical NICs.
I	Compromised Systems	Investigate each guest OS for compromise during normal scanning for malware.
J	Monitoring of Communication	Monitor the security of activity occurring between guest OSs.

4.4 Secure Virtualization Planning and Deployment

The security of a virtual environment should be factored into the entire system development lifecycle, from planning to deployment, to maximize effective security and minimize the cost of security. For further information on system development lifecycle security requirements see *Configuration Management Policy*. For further information and guidance on virtualization-specific system development lifecycle security practices, see NIST 800-125 “Guide to Security for Full Virtualization Technologies”.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy, then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency’s mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Auditing and Compliance Policy
- Configuration Management Policy
- Incident Response Policy
- Patch Management Policy

7.0 Definitions

Term	Definition
Confidential Information	Confidential information is non-public information and is defined by 3 sub-categories: (1) Personally Identifiable Information; (2) Privileged Information; and (3) Sensitive Information. More information regarding Confidential Data can be found in the *DoIT Public and Confidential Policy*.
Full-virtualization	A form of virtualization where one or more operating systems and the applications they contain are run on top of virtualized hardware. There are two main types: (1) Native (or bare-metal) virtualization (2) Hosted virtualization
Guest Operating System (Guest OS)	A virtual guest or virtual machine (VM) that is installed under the host operating system.
Host Operating System	In a hosted virtualization solution, the OS that the hypervisor runs on top of.
Hosted Virtualization	A form of full virtualization where the hypervisor runs on top of a host OS.
Hypervisor	Also known as a Virtual Machine Monitor. The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.
Native Virtualization	Also known as a Bare-Metal Virtualization. A form of full virtualization where the hypervisor runs directly on the underlying hardware, without a host OS.
Operating System (OS)	A system software that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.
Virtualization	The simulation of the software and/or hardware upon which other software runs.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for ensuring the security of virtualized technology within the Enterprise. Agencies not directly managed by DoIT must comply with the requirements detailed in section 4.0 unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies must manage virtual environment security to ensure that data is protected from breach or loss.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be considered a security violation and subject to investigation and possible disciplinary action, which may include written reprimand, suspension, termination, and possible criminal and/or civil penalties